UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073

26889 7590 10/15/2007

MICHAEL CHAN
NCR CORPORATION
1700 SOUTH PATTERSON BLVD
DAYTON, OH 45479-0001

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 09/651,979
Filing Date: August 31, 2000
Appellant(s): SHIELDS, ADRIAN

Gregory A. Welte
(Reg. No. 30,434)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 07/16/2007 appealing from the Office action mailed 08/28/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 21-34 and 38 are rejected under 35 USC 103 over Yacobi in view of Menezes.

Claims 35-37 are rejected under 35 USC 103 over Yacobi, Menezes and further in view of Kawan.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5878138	YACOBI	3-1999
20020062284	KAWAN	5-2002

Menezes, Alfred A. et al., "Handbook of Applied Cryptography" CRC Press, 1997, pp. 170-172, 494, and 552.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 21-34 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yacobi (US 5878138) in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 21 and 33, Yacobi discloses a portable computer, with non-secure user-accessible memory (see column 8 lines 39-49) generating a session key (see column 9 line 47); encrypting the session key (see column 9 lines 49-50);

transmitting the encrypted key to an external terminal (see column 9 lines53-54); receiving and decrypting an encrypted response from the terminal (see column 9 line 65 through column 10 line 31).

Yacobi fails to disclose a) storing records of events experienced by the computer in memory within the computer; and using some of the records as seed for generating plain text of a first session key K1.

However, Menezes et al teaches storing records of events and using the records as a seed for generating a key (see page 172).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's key generation to generate the session key of Yacobi.

Motivation to do so would have been to generate a random bit sequence for a key (see page 171).

As per claims 22, 24, 26-30, and 38, the modified Yacobi and Menezes et al system further includes repeating the above mentioned steps to create a new session key for each new transaction (see Yacobi column 10 lines 38-47) and receiving and decrypting encrypted messaged encrypted by the session key (at both the portable computer and the external device) (see Yacobi column 9 line 65 through column 10 line 31).

As per claims 23, 25, 31-32, and 34, the modified Yacobi and Menezes et al system further includes the data used as the seed includes at least one element selected from the following group: recorded button selections, recorded pointer movements, recorded data entered by a user, current date setting, and current time setting (see Menezes page 172).

Claims 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Yacobi and Menezes et al system as applied to claims 21, 24, and 26 above, and further in view of Kawan (US 20020062284)..

As per claims 35-37, the modified Yacobi and Menezes et al system fails to include the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN

However, Kawan teaches the requirement of a PIN (see paragraph 30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to require a PIN to perform the actions of the modified Yacobi and Menezes system.

Motivation to do so would have been to verify the user (see paragraph 30).

(10) Response to Argument

Rejection of claims 21-34 and 38 under 35 U.S.C. 103(a) as being unpatentable over Yacobi in view of Menezes

Claim 21

Appellant argues that Yacobi fails to disclose, "de-crypting the encrypted response using the plain text of K1."

With respect to this Argument, Yacobi discloses generating a symmetric session key (i.e. K1) in column 9 lines 47-49 and further discloses the establishment of a secure channel using an encryption key (i.e. the session key) in column 10 lines 1-5. Therefore, for the channel to be secure the messages are encrypted before they are sent and decrypted when they are received. Since the session key is "symmetric" the same value is used as the key for both encryption and decryption. Furthermore, in column 10 lines 7-9 the user requests, over the secure channel, withdrawal of electronic cash. In response, the bank generates digital coins (see column 10 lines 9-31). The coins are then sent over the secure channel to the users electronic wallet (i.e. the encrypted response) (see column 10 lines 32-33). The coins are then available for the user to obtain service from a merchant (see column 10 lines 38-56). Since the coin is shown to be in original form before signing and sending to the merchant the coin sent over the secure channel (i.e. encrypted) must be decrypted by the wallet. The secure channel that is established uses a symmetric session key so the encrypted response is decrypted using the same value as the key that encrypted it. Therefore, Yacobi discloses "decrypting the encrypted response using the plain text of K1."

In response to Appellant's specific argument, POINT 1, that the encrypted hash value cannot correspond to the encrypted response; the hash value is signed by encrypting it with the bank's private key and then sent over the secure channel (i.e. encrypted) in response to a request by the user. Therefore, the encrypted signed hash value is the claimed "encrypted response".

In response to Appellant's specific argument, POINT 2 and POINT 3, that there is no decrypting of the encrypted hash; as stated above, the digital coin (i.e. the signed hash value) is encrypted (i.e. sent over the secure channel) and the plain value of the digital coin is used with a merchant so the encrypted digital coin must be decrypted. Therefore, Yacobi discloses decrypted an encrypted response.

In response to Appellant's specific argument, POINT 4, that the session key is not involved in the encryption of the hash value of the digital cash and therefore cannot be used for any decryption; as stated above, the session key is used to create the secure channel by encrypting the messages sent between the wallet and the bank during a session. Therefore, when the signed hash value, the digital cash, is sent from the bank to the wallet the session key is used to encrypt the cash at then bank and decrypt it as the wallet.

In response to Appellant's specific argument, POINT 5, that the processing is done outside the wallet (which is portable, see column 8 lines 39-49), the session key used to create the secure channel is generated in the wallet (see column 9 lines 47-49) and all communication between the wallet and the bank are done over the secure channel (see column 10 lines 7-9 and lines 32-33) so the wallet does all the encryption and decryption. Therefore, the processing is not done outside the wallet.

Appellant's argument that Menezes fails to make up for the cited deficiencies of Yacobi is moot in view of the above response.

Appellant argues that there is no teaching given for combining Menezes with Yacobi.

With respect to this argument Yacobi teaches generating a session key (see column 9 lines 47-49), but does not disclose how the key is generated. Menezes teaches a well-known method of using events experienced by the computer as a seed to generate a random bit sequence used as a key (see page 172 section (ii)). Since both references teach methods of generating keys, it would have been obvious to one of ordinary skill in the art to substitute one method for the other to achieve the predictable result of a generated key.

In response to Appellant's specific argument, Problem 1, that the keys in both Yacobi and Menezes are inherently random and therefore the statement does not lead to a combination of the references, key *should* be random but the mere use of a key does not mean it is inherently random. Therefore, the motivation to generate a random bit sequence for a key is valid. Furthermore, Menezes teaches the additional advantageous feature of distilling the random bits from the sampled sequences.

In response to Appellant's specific argument, Problem 2, that the other sources of random values and there is no motivation to select one over the others; the section relied upon for this teaching was the Software-based generators section and each of the listed processes, in which a random bit sequence may be derived, related to the claimed invention and any or all of them can be used. Therefore there is no need to provide motivation for using one over the other.

In response to Appellant's specific argument, Problem 3, that Menezes teaches away from storing the records in user-accessible memory; Menezes does not teach where the values should be stored, therefore when combined with Yacobi whole only teaches user-accessible memory (see column 8 lines 39-42) the records must be stored in this memory. Furthermore, Applicant argues that "The generator must not be subject to observation." However, Menezes does not explicitly state this, as Applicant's quotation would imply. Menezes teaches that the recorded events should be protected against observation and provides a solution where the events (i.e. records) are collected, concatenated into one value (i.e. the seed) and then run through a hash function to obtain the random bit sequences. Therefore, Menezes does not teach away from storing the records in user-accessible memory.

Appellant argues, see Problem 4, that there are two possible ways to generate the random bit sequence of Menezes, one using memory and one that does not require memory. With respect to this argument Menezes teaches the concatenation of sampled sequences, in order for a computer to concatenate values it must store each of the values in memory in order to add one value to the end of another. Even in Appellant's example, see Possibility 2, in order to use each of the four values given as a seed he must remember (i.e. store) each value in order to use the combination of them as a seed. Therefore, Menezes method of generating a random bit sequence cannot be performed without the use of memory.

In response to Appellant's specific argument, Problem 5, that Menezes teaches two different generation methods and there is no teaching to choose one over the other, Menezes discloses two different methods for generating random bit sequences (hardware and software based methods) and provides advantages and disadvantages for using both methods. One of ordinary skill in the art would recognize that using a hardware-based method would not be advantageous in the system of Yacobi because it requires additional (external) hardware not suited for the small portable device of Yacobi (the device described in column 8 lines 39-49). While the software approach may be "more difficult" it still has the advantage of not requiring the additional hardware. Therefore, Menezes does teach advantages of choosing software-based generation over hardware-based generation.

In response to Appellant's specific argument, Problem 6, that the Examiner has given no teaching to select a first embodiment of Yacobi instead of a second embodiment; the first embodiment more closely relates to the claimed invention and is additionally receptive to a combination with Menezes.

Claims 22 and 23

Appellant's argument that claims 22 and 23 are patentable based on their parents is moot in view of the above response.

Claim 24

Appellant argues that the combined references fail to disclose encrypting two keys using a public key and transmitting the encrypted key to an external terminal.

With respect to this argument, Yacobi teaches generating a session key, encrypting the session key with the public key of the bank and transmitting the encrypted session key to the bank (see column 9 lines 47-54). This process is performed each time the user requests digital cash with a new session key generated each time, as evidenced by Menezes page 494 where a session key is only used for one session. In Yacobi one session is the request and delivery of digital cash. Therefore, the cited references disclose encrypting two keys using a public key and transmitting the encrypted key to an external terminal.

Appellant's arguments that Menezes fails to teach producing keys from user-accessible memory and lack of motivation to combine are moot in view of the above response.

Claim 26

Appellant's arguments, see Points 1-4, have been addressed above with respect to claim 21 and are therefore moot.

Claim 27

Appellant argues that Yacobi fails to disclose decrypting the second encrypted message with the second key K2.

With respect to this argument, as discussed with respect to claim 24, Yacobi teaches a second key K2. Additionally when the bank delivers the digital cash, after the second request, it is encrypted with the second session key (i.e. K2). As addressed with respect to claim 21 the encrypted digital cash is then decrypted with the session key (K2). Therefore, Yacobi discloses decrypting the second encrypted message with the second key K2.

Appellant's argument that Menezes lacks of motivation to combine is moot in view of the above response.

Claims 28 and 30

Appellant argues that Yacobi teaches away from an apparatus with "no secure area" for storing an encryption key because Yacobi teaches the device is tamper-resistant.

With respect to this argument Yacobi's reference to "tamper-resistant" is with respect to reverse engineering the device (see column 2 lines 12-23) and not the accessibility of the contents of the device. All of the memory is accessible to the valid user of the device and therefore not secured. Additionally, from the description in column 2 it is clear that for the device to be secured it must be tamper-proof and not merely tamper-resistant. Therefore, Yacobi does not teach away from an apparatus with "no secure area" for storing an encryption key.

Appellant's argument that Menezes lacks of motivation to combine is moot in view of the above response.

Claims 32, 33, and 38

Appellant's arguments with respect to these claims have been addressed above with respect to claim 21 and are therefore moot.

Rejection of claims 35-37 under 35 U.S.C. 103(a) as being unpatentable over Yacobi in view of Menezes and further in view of Kawan

Appellant argues that Kawan fails to disclose requiring a PIN to be entered into the portable computer or a transaction will not be completed.

With respect to this argument, while paragraph 30 of Kawan may be ambiguous as to whether the PIN is entered into the PDA or ATM, claims 35-37 are as ambiguous. Specifically, these claims require the entry of a PIN and will not complete the transaction without the PIN. Therefore, if the PIN is not entered into either the PDA or the ATM of Kawan no transaction will occur.

Therefore, Kawan teaches the limitations of claims 35-37. Additionally, assuming arguendo, that the claims require the PIN to be entered into the PDA, paragraphs 28 and 31 teach this limitation because the PIN is pre-stored in the PDA and therefore must have been entered in the PDA.

Appellant argues that there is no teaching for combining the references and presents four "Problems".

With respect to Problem 1, Appellant argues that the PIN is entered into the portable computer. However, as addressed the claims do not explicitly require this limitation. Even if these claims required the PIN be entered into the portable computer Kawan teaches this in paragraphs 28 and 31.

With respect to Problem 2, Appellant argues that there are numerous ways to verify a user and the Examiner has not shown why a PIN should be used as opposed to one of the other methods. In response to this argument, some motivation must be presented to show why one of ordinary skill in the art would make the proposed motivation. In this case, one would want to use a PIN in order to verify a user. While other methods of verifying a user may be available, one must only show motivation to use a PIN.

With respect to Problem 3, Appellant argues that the combination is in contradiction to Yacobi because Yacobi requires entering a PIN onto an ATM keypad. However, Yacobi never states that a PIN number is entered onto an ATM keypad. The cited portion (column 5 line 35) merely states that a transaction can be conducted "over a private banking network (e.g., ATM -automatic teller machine)". Furthermore, Yacobi never even mentions a PIN therefore this argument is irrelevant.

With respect to Problem 3, Appellant argues that the Yacobi reference teaches verifying the user using traditional methods, which implies entering a PIN into an ATM and therefore teaches away from entering a PIN into the portable device. However, as stated above Yacobi never discloses the use of a PIN for user verification. Additionally, Yacobi teaches in column 9 lines 3-6, "the electronic wallet…submits the key pair along with user identification to the bank's computer". Therefore, contrary to Appellant's statement the user information is sent from the portable device not at an ATM and the user verification must be entered into the portable computer for it to send the information to the bank computer. Therefore, Yacobi does not teach away from entering a PIN into the portable device.

Rebuttal of Final Action's "Response to Arguments"

Each of the points presented in this section have been addressed above and therefore are moot.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael J. Pyzocha

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron

Matthew Smithers

/Matthew Smithers/
Primary Examiner
Art Unit 2137